CLAIMS

What is claimed is:

1. A method comprising:

stalling a file system event, said file system event including a file name;

parsing said file name to obtain at least a last file name extension of said file name;

determining whether said last file name extension is the only file name extension of said file name;

upon a determination that said last file name extension is not the only file name extension of said file name, determining whether said last file name extension is a dangerous file name extension; and

upon a determination that said last file name extension is a dangerous file name extension, generating a notification.

2. The method of Claim 1, further comprising:

implementing protective actions.

3. The method of Claim 1, further comprising:

terminating said file system event.

4. The method of Claim 1, further comprising:

intercepting said file system event.

5. The method of Claim 4, wherein said file system event originates from a selected category of applications.

6. The method of Claim 5, wherein said selected category of applications is a network application.

7. The method of Claim 4, wherein said file system event originates from an instant messaging application.

8. The method of Claim 4, wherein said file system event originates from an electronic mail (e-mail) application.

9. The method of Claim 4, wherein said file system event originates from a peer-to-peer (P2P) network application.

10. The method of Claim 1, further comprising:
obtaining said file name from said file system event.

11. The method of Claim 1, wherein said parsing said file name further obtains at least a next to last file name extension of said file name.

12. The method of Claim 1, wherein upon a determination that said last file name extension is the only file name extension of said file name, said method further comprising:
releasing said file system event.

13. The method of Claim 1, wherein upon a determination that said last file name extension is not dangerous, said method further comprising:
releasing said file system event.

14. The method of Claim 1, further comprising:
prior to said determining whether said last file name extension is a dangerous file name extension, determining whether a by-pass option is selected, wherein selection of said by-pass option by-passes said determining whether said last file name extension is a dangerous file name extension when said last file name extension is visible to a user; and
upon a determination that said by-pass option is selected, determining whether said last file name extension is visible to a user.

15. The method of Claim 14, wherein upon a determination that said last file name extension is not visible to a user, said method further comprising:

performing said determining whether said last file name extension is a dangerous file name extension.

16. The method of Claim 14, wherein upon a determination that said last file name extension is visible to a user, said method further comprising:

not performing said determining whether said last file name extension is a dangerous file name extension; and

releasing said file system event.

17. The method of Claim 14, wherein upon a determination that said by-pass option is not selected, said method further comprising:

performing said determining whether said last file name extension is a dangerous file name extension.

18. The method of Claim 11, wherein said determining whether said last file name extension is a dangerous file name extension comprises:

determining said last file name extension;

determining whether said last file name extension is an executable file name extension;

upon a determination that said last file name extension is an executable file name extension, determining said next to last file name extension;

determining whether said next to last file name extension is a registered file name extension;

upon a determination that said next to last file name extension is a registered file name extension, determining whether said next to last file name extension is an excluded file name extension; and

upon a determination that said next to last file name extension is not an excluded file name extension, determining that said last file name extension is dangerous.

19. The method of Claim 18, wherein upon a determination that said last file name extension is not an executable file name extension, said method further comprising:

releasing said file system event.

20. The method of Claim 18, wherein said determining whether said last file name extension is an executable file name extension, comprises:

comparing said last file name extension to one or more entries of executable file name extensions in an executable file name extension list to determine whether said last file name extension matches at least one of said one or more entries of executable file name extensions;

upon a determination that said last file name extension matches said at least one of said one or more entries of executable file name extensions, determining said last file name extension is an executable file name extension; and

upon a determination that said last file name extension does not match said at least one of said one or more entries of executable file name extension, determining said last file name extension is not an executable file name extension.

21. The method of Claim 18, wherein said determining whether said last file name extension is an executable file name extension, comprises:

locating a file associated with said file name;

opening said file to access the contents of said file;

examining said contents to determine whether said file is an executable file;

wherein upon a determination that said file is an executable file, determining said last file name extension is an executable file name extension; and

wherein upon a determination that said file is not an executable file, determining said that said last file name extension is not an executable file name extension.

22. The method of Claim 18, wherein upon a determination that said next to last file name extension is not a registered file name extension, said method further comprising:

determining that said last file name extension is not dangerous.

23. The method of Claim 18, wherein upon a determination that said next to last file name extension is an excluded file name extension, said method further comprising:

determining that said last file name extension is not dangerous.

24. A system comprising:

an anti-viral application, said anti-viral application for intercepting and stalling a file system event including a file name; and

a detection application communicatively coupled to said anti-viral application, said detection application for detecting a dangerous file name extension present in said file name.

25. The system of Claim 24, wherein said anti-viral application is a behavior blocking application.

26. The system of Claim 24, wherein said anti-viral application comprises:

an intercept module for intercepting and stalling said file system event including said file name.

27. The system of Claim 24, wherein said detection application comprises:

a parsing module for obtaining said file name and for parsing said file name to obtain at least a last file name extension, and a next to last file name extension, when present, of said file name;

a logic module for determining whether said last file name extension is a dangerous file name extension; and

a found file name extension(s) list for storing at least said last file name extension and said next to last file name extension, when present.

28. The system of Claim 24, wherein said anti-viral application further comprises:

an executable file name extension list;

a file name extension registry; and

an exclusion list.

29. The system of Claim 27, wherein said detection application further comprises:

an executable file name extension list;

a file name extension registry; and

an exclusion list.

30. A computer program product comprising a computer-readable medium containing computer program code for a method comprising:

stalling a file system event, said file system event including a file name;

parsing said file name to obtain at least a last file name extension, and a next to last file name extension, when present, of said file name;

determining whether said last file name extension is the only file name extension of said file name;

upon a determination that said last file name extension is not the only file name extension of said file name, determining whether said last file name extension is a dangerous file name extension; and

upon a determination that said last file name extension is a dangerous file name extension, generating a notification.

31. The computer program product of Claim 30, said method further comprising:

implementing protective actions.

32. The computer program product of Claim 30, said method further comprising:

terminating said file system event.

33. The computer program product of Claim 30, wherein said determining whether said last file name extension is a dangerous file name extension comprises:

determining said last file name extension;

determining whether said last file name extension is an executable file name extension;

upon a determination that said last file name extension is an executable file name extension, determining said next to last file name extension;

determining whether said next to last file name extension is a registered file name extension;

upon a determination that said next to last file name extension is a registered file name extension, determining whether said next to last file name extension is an excluded file name extension; and

upon a determination that said next to last file name extension is not an excluded file name extension, determining that said last file name extension is dangerous.